

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE**

**IN THE MATTER OF THE SEARCH)
AND SEIZURE OF A SAMSUNG A14)
CELLULAR, TELEPHONE)
CURRENTLY IN THE CUSTODY OF)
U.S. PROBATION & PRETRIAL)
SERVICES, 55 PLEASANT STREET,)
CONCORD, NEW HAMPSHIRE)**

Case No. 23-mj-220-01-TSM

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant authorizing the seizure and search of a Samsung A14 cellular telephone with assigned number 603-497-1163, which was seized from Philip LONGEWAY and currently in the custody of U.S. Probation & Pretrial Services, 55 Pleasant Street, Room 211, Concord, New Hampshire 03301 (“the Device”). I seek authority to seize and search the Device and extract from it electronically stored information that constitutes evidence, fruits, and instrumentalities of criminal violations which relate to the distribution of child pornography, as described in Attachment B.

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including

those relating to child exploitation, child pornography, and human trafficking. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

2. I am a “Federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the Devices.

4. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(2) (receipt/distribution of child pornography) have been committed by Philip Longeway and that there is probable cause to believe that evidence and fruits, and instrumentalities of violations of that crime, as set forth below, will be found on the Device.

STATUTORY AUTHORITY

5. This investigation concerns an alleged violation of 18 U.S.C. § 2252(a)(2), related to the receipt/distribution of child pornography in the District of New Hampshire. Section 2252(a)(2) makes it a crime for any person to knowingly distribute any visual depiction using any means or facility of interstate or foreign commerce if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

6. “Child pornography” includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

7. “Sexually explicit conduct” is defined by 18 U.S.C. § 2256(2)(A) as “actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal . . .; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.”

8. Not every display of the genitals or pubic area qualifies as “lascivious exhibition.” In deciding whether the display of the genitals or pubic area is a “lascivious exhibition,” the following factors may be considered: (1) whether the genitals or pubic area are the focal point of the display; (2) whether the setting is sexually suggestive, for example, a setting traditionally associated with sexual activity; (3) whether the child’s pose is unnatural or her attire

inappropriate, taking her age into consideration; (4) whether the child is fully or partially nude; (5) whether the display suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the display appears designed or intended to elicit a sexual response from the viewer.

9. “Minor” means any person under the age of 18 years. 18 U.S.C. § 2256(1).

10. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

PROBABLE CAUSE

11. In November 2023, U.S Probation Officer, Location Monitoring Specialist, Matthew Senesi of the United States Probation and Pretrial Services (USPPS) in the District of New Hampshire, provided your affiant with the following information.

12. On March 20, 2006, the Court sentenced Philip Longeway on a charge of Travel with Intent to Engage in Illicit Sexual Conduct. The Court imposed a 210-month term of imprisonment and lifetime supervised release.

13. IPPC software is the name of a software company contracted by the United States Probation Office to conduct computer monitoring of persons under supervision. Prior to contracting with IPPC, the Probation Office contracted a different company, RemoteCom, that provided monitoring software. Both companies employ staff and uses software to monitor certain activity that may be captured by a monitored computer (the “monitoring software”), and it populate an online database with content such as screenshots for U.S. Probation Officers to view.

14. In or around November 2019, RemoteCom monitoring software was installed on Longeway's smartphone.

15. On or about June 29, 2023, after the Probation Office contracted with IPPC, IPPC monitoring software was installed on Longeway's smartphone (the "Device").

16. On September 20, 2023, U.S. Probation Officer Matthew Senesi, submitted a petition for a warrant and revocation of Longeway's supervised release based on information captured by the monitoring software.

17. On September 21, 2023, the Probation Officer withdrew the petition for a warrant and requested that IPPC deactivate the monitoring software after determining that Longeway's conditions of release did not include a computer monitoring condition.

18. On October 17, 2023, the Probation Officer submitted a Request for Modifying the Conditions or Term of Supervision with Consent of the Offender. That document requested that the Court add the following special conditions of supervised release, which the Court approved on October 19, 2023:

To ensure compliance with the computer monitoring condition, you must allow the probation officer to conduct initial and periodic unannounced searches of any computers (as defined in 18 U.S.C. § 1030(e)(1)) subject to computer monitoring. These searches shall be conducted for the purposes of determining whether the computer contains any prohibited data prior to installation of the monitoring software; to determine whether the monitoring software is functioning effectively after its installation; and to determine whether there have been attempts to circumvent the monitoring software after its installation. You must warn any other people who use these computers that the computers may be subject to searches pursuant to this condition. You must allow the probation officer to install computer monitoring software on any computer (as defined in 18 U.S.C. § 1030(e)(1)) you use. You must pay for the cost of this monitoring software to the extent you are able, as determined by the probation officer.

19. After the Court approved the special condition, the Probation Officer requested that IPPC reactivate the monitoring software.

20. According to U.S. Probation Officer Matthew Senesi, on October 20, 2023, Longeway deactivated the IPPC monitoring software from the Device. After a conversation with the Probation Officer, on October 30, 2023, Longeway called IPPC to reactivate the monitoring software on the Device.

21. As laid out in more detail below, on November 3, 2023, at 7:44 pm, the monitoring software captured Longeway communicating with an individual who stated he was 15 years old. Approximately one hour later, the monitoring software captured screenshots of the alleged minor masturbating for the defendant on the Zoom video conference application.

22. After the video call, the monitoring software captured a text message exchange between Longeway and the alleged minor in which Longeway said, "If I'm able to get down there in a week or two we're going to have to figure something out". On November 5, 2023, at 10:31 am, Longeway and the self-identified minor conducted a Zoom video call where the male again masturbated for Longeway.

23. Based on my training and experience I know that individuals can take and store "screen shots" of images or video displayed on the screen of their smartphone. Based on my training and experience I also know that Zoom allows users to make video recordings of Zoom sessions and store them on their electronic devices.

24. On November 7, 2023, IPPC notified the Probation Officer of the incidents. The Probation Officer then checked the IPPC database and confirmed that screenshots of Longeway's smartphone (the Device) showed that he communicated with the self-identified minor via text and video conference during the above period.

25. On November 13, 2023, Assistant United States Attorney (AUSA) Matthew Hunter requested that I review the information captured by the monitoring software to determine if it warranted a criminal investigation.

26. On November 15, 2023, I met with U.S. Probation Officer Senesi at his office in Manchester, NH. To authorize my review of his case file, U.S. Probation Officer Senesi submitted a Request to Disclose Supervision Case File Information to U.S. District Court Judge Stephen J. McAuliffe. On or about November 20, 2023, Judge McAuliffe granted that request.

27. On November 16, 2023, the Probation Officer met with Longeway at his residence. During that meeting, the Probation Officer seized Longeway's phone. Longeway admitted to the Probation Officer that he had used his phone to communicate with an individual he believed to be a minor. He admitted that he watched the alleged minor masturbate on the Zoom video application on two occasions. The following day, the probation officer completed a Petition for Warrant or Summons for Offender Under Supervision, citing four violations of supervised release.

28. On November 28, 2023, I met with U.S. Probation Officer Senesi who provided copies of Case File Information regarding Philip Longeway. I reviewed the Case File Information with U.S. Probation Officer Senesi and noted the following.

29. According to Probation Officer Senesi, Longeway stated that he met the victim using a smartphone application called "BoyAhoy." I researched publicly available information concerning the "BoyAhoy" application, which indicated that "BoyAhoy" represents itself to be a free global network application for meeting gay men.

30. I also reviewed short message service (SMS) or text message communications and images between Philip Longeway and another individual that had been captured from

Longeway's phone. I reviewed communications captured between November 2, 2023, at 7:33am and November 16, 2023, at 3:52am.

31. The messages I reviewed were between Longeway and an individual who stated he was 15 years old (the "Minor"). In the messages, the Minor is initially referred to himself as "Sam" but later told Longeway his actual name is "Sah".

32. According to sender and receiver information in the messages, Longeway was communicating from the telephone number 603-497-1163 (the Device) and the Minor was communicating from the telephone number 856-577-1048.

33. I have reproduced below examples of messages I reviewed between Longeway and the Minor.

34. The messages sent by Longeway's phone number identify the sender as "me." Initially, the messages sent by the Minor showed only his phone number but later messages show the Minor's phone number associated with contact "Sah." Based on my training and experience this indicates that Longeway added "Sah" as a contact in the address book on his phone.

35. In the examples reproduced below, I have identified "Minor" as the sender of messages sent from the telephone number 856-577-1048 and I have identified "Longeway" as the sender of messages sent from the telephone number 603-497-1163.

36. On November 3, 2023, between 6:38pm and 6:50pm, the below messages were sent and received from the Device:

Minor: I have to tell you sum don't get mad Tho
Longeway: Okay
Longeway: I'm ready for you to tell me I won't get mad
Minor: The pic thts on the profile
Longeway: I'm very open-minded
Minor: It wasn't me
Longeway: Okay how old are you and what do you look like
Longeway: Come on now don't be scared

Minor: I'm not
Minor: To be honest
Minor: I'm 15 bout to be 16 and I'll send you pics (blowing kiss emoji)
Longeway: Well then let me see you
Minor: I ammmmm
Minor: Ok (thumbs up emoji)
Longeway: Okay
Longeway: Snap me a regular picture of your face so I can see your face without moving around cuz I think you're cute
Longeway: Do you want to be with an older guy
Longeway: where'd you go sexy
Minor: Yess I like older guys
Minor: But do you like younger guys ????
Longeway: Yeah that's actually what I want
Minor: Look at the first video it's shows my face
Longeway: I know well I'm driving right now that's why I asked you to do that
Longeway: Where are you from again cuz I'm in New Hampshire
Minor: Dang I'm in Camden
Minor: Camden New Jersey
Longeway: Don't give up there's always a chance I could come on a weekend
Longeway: I think I would love making out with you and feeling you up let you have your way with me

37. On November 3, 2023, between 7:30pm and 7:47pm the below messages were sent and received from the Device:

Minor: Do you have zoom?
Longeway: Yeah I have zoom why what do you want to do
Longeway: I don't have an account I just have it
Longeway: I have WhatsApp
Longeway: I will be going to sleep soon cuz I have to get up at 1:00 in the morning for work
Longeway: I'll be home around 10:00 a.m. tomorrow
Longeway: So if we're trying to look at each other let's do it
Minor: Ok
Minor: Put in 618 661 8849 rVV1WX
Longeway: Ok

38. After these messages, I saw 16 still images captured by the monitoring software from the Zoom video. The still images depict a pubescent black male. Of those, 14 images depict a nude minor with an erect penis visible. Some of the images also depict seminal fluid on

the males erect penis, consistent with masturbation to ejaculation. The minor appears to be in a bathroom, as a shower/shower curtain is visible. Longeway's face/shoulders are depicted in a smaller screen within the images. In the screen capture, Longeway has black rimmed glasses and appears to have no shirt on.

39. USPO Senesi reviewed the screen captured images and identified Longeway.

40. According to the chat and screen captures, after the Zoom session, Longeway sent the below messages from the Device:

Longeway: You are hot I want to kiss you I want to love you I want to be with you oh my God. I'm going to go to bed night thinking about you all night. You are so sexy and sweet. If I'm able to get down there within a week or two we're going to have to figure something out.

Longeway: Good night you know my name is Philip right

41. On November 5, 2023, between 10:17am and 10:52am, the below messages were sent and received from the Device:

Minor: Want to do it again

Longeway: I would love to are you horny right now I'm in my car I'll have to wait until I get home

Longeway: I want you to do it in my mouth

Longeway: Will you show me your hole

Longeway: I wish I could taste it

Minor: Yes to all lol

Minor: I'm very horny

Longeway: So you doing that in front of me makes you come better

Longeway: If I was with you I'd let you fuck me

Minor: Fuck yea

Longeway: Do you want me to watch while I'm sitting in my car waiting till I get home so I can jerk

Longeway: I can do it in my car and then I'll jerk later on

Longeway: Cuz I'm waiting for a store to open

Minor: Yesss

Longeway: Okay let's go I'll jerk later on

Longeway: You'll have to send me the link again

Longeway: I just need the password

Minor: rVV1WX

Minor: 618 661 8849

Minor: Don't be Lund
Minor: Loud *
Longeway: Okay

42. After these messages, I saw 13 still images captured by the monitoring software from the Zoom video. The still images depict a pubescent black male. Of those, 11 images depict a minor wearing only a blue sweatshirt with an erect penis visible. Some of the images also depict seminal fluid on the male's erect penis, consistent with masturbation to ejaculation. The minor appears to be in a bathroom, as a shower/shower curtain is visible. Longeway's face/shoulders are depicted in a smaller screen within the images. In the screen capture, Longeway has black rimmed glasses and appears to have a multi-colored sweatshirt on.

43. USPO Senesi reviewed the screen captured images and identified Longeway.

44. According to the chat and screen captures, after the Zoom session, the below messages were sent and received from the Device:

Longeway: I want to taste you one day did it feel good
Longeway: I want to put my tongue in your ass and then have you fuck me real good
Longeway: If I was with you I would do anything you want
Longeway: I will swallow every drop of your cum
Minor: Nice (thumbs up emoji)
Minor: My cum got all over my phone
Longeway: I wish you'd get it all over my face

45. In later messages between Longeway and the Minor, the Minor asked Longeway for money and provided his CashApp information. Longeway replied that he would "do something when I get paid Thursday morning" and "You're worth it."

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS OR PRODUCE
CHILD PORNOGRAPHY

46. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who view and/or possess, receive, and/or produce images of child pornography:

- a. Individuals who possess, receive, and/or produce child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity. Individuals who have a sexual interest in children or images of children typically retain such images for many years.
- b. Likewise, individuals who possess, receive, and/or distribute child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer or smartphone. These child pornography images are often maintained for several years and are kept close by, to enable the individual to view the child pornography images, which are valued highly.
- c. Individuals who possess, receive, and/or distribute child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Forums, such as chat

rooms, bulletin boards, newsgroups or IRC chat rooms have forums dedicated to the trafficking of child pornography images.

d. Individuals who interact with minor victims through live streaming on the internet, using platforms like Zoom, will commonly memorialize these interactions by saving media files (such as still images, videos) on their devices.

47. I know, based on my training and experience, that people who have a demonstrated sexual interest in children and child pornography often maintain collections of images of child pornography. I am therefore requesting authority to search the Devices for evidence of child pornography or any communication involving the abuse of children, and evidence relating to the production, possession, and distribution of any child pornography or child exploitation material.

48. As with most digital technology, communications made from a computer or cellular phone are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded

to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

49. I also know that electronic devices store evidence that can inform investigators who used the Device, when, and how it was used.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

50. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

51. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

52. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

53. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

54. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

55. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

56. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

57. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

58. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

59. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

60. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

61. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

62. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

63. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

64. Based on the foregoing, there is probable cause to believe contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252 (receipt/distribution of child pornography) will be found on the Devices described in Attachment A. I respectfully request that this Court issue a search warrant for the Devices, authorizing the seizure and search of the items described in Attachment B.

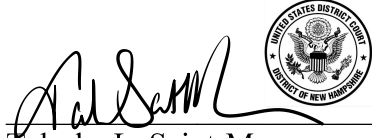
/s/ Ronald Morin

Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Dec 6, 2023**

Time: **2:34 PM**

A handwritten signature in black ink, appearing to read 'Talesha L. Saint-Marc', is written over a horizontal line.

Talesha L. Saint-Marc
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

The property to be seized and searched includes a Samsung A14 cellular telephone with assigned telephone number 603-497-1163, seized from Philip Longeway on November 16, 2023 by U.S. Probation and Pretrial Services, and currently in the custody of U.S. Probation and Pretrial Services, 55 Pleasant Street, Room 211, Concord, New Hampshire 03301 (“the Device”).

This warrant authorizes the seizure and forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Device described in Attachment A that relate to violations of 18 U.S.C.

§ 2252(a)(2) (receipt/distribution of child pornography) including:

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, electronic messages, or other digital data files) pertaining to the distribution, production and possession of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
2. In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8), child exploitation material, visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), images or videos of children showering or using the bathroom, or child erotica.
3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the owner of the Devices for the purpose of receiving, sending, or discussing child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.
5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
6. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to use or ownership of the Device described above.

7. Any and all documents, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.